What is claimed is:

1. A method for securing an accessible computer system, the method comprising:

monitoring a computer system for connection transactions between at least one access requestor and at least one access provider; and

denying access by the access requestor to the access provider when a number of connection transactions initiated by the access requestor exceeds a configurable threshold number during a first configurable period of time.

2. The method as in claim 1, wherein the monitoring includes detecting connection transactions initiated by the access requestor.

3. The method as in claim 2, wherein the monitoring further includes counting the number of connection transactions initiated by the access requestor during the first configurable period of time.

4. The method as in claim 3, wherein the monitoring further includes comparing the number of connection transactions initiated by the access requestor during the first configurable period of time to the configurable threshold number.

5. The method as in claim 1, wherein the monitoring includes detecting connection transactions between at least one Internet protocol address and the access provider.

6. The method as in claim 5, wherein the monitoring further includes counting the number of connection transactions initiated by the Internet protocol address during the first configurable period of time.

7. The method as in claim 6, wherein the monitoring further includes comparing the number of connection transactions initiated by the Internet protocol address during the first configurable period of time to the configurable threshold number.

8. The method as in claim 6, wherein the monitoring includes monitoring a computer system for connection transactions made using TCP.

9. The method as in claim 5, wherein the detecting includes identifying the Internet protocol address through the use of a header attached to a message representing the connection transaction being detected.

10. The method as in claim 1, wherein the denying of access includes denying access to the access provider by the access requestor for a second configurable period of time.

11. The method as in claim 10, wherein the denying of access further includes resetting the second configurable period of time after detecting a new connection transaction initiated by the access requestor during the second configurable period of time.

12. The method as in claim 1, wherein the denying of access includes denying access to the access provider by the access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

13. The method as in claim 1, wherein the access requestor is a client and the access provider is a host such that the monitoring includes detecting connection transactions between at least one client and at least one host.

14. The method as in claim 1, wherein the access requestor is a client and the access provider is a host such that the monitoring includes detecting connection transactions between the access requestor and a plurality of access providers.

15. A system for securing an accessible computer system, comprising:

means for monitoring a computer system for connection transactions between at least one access requestor and at least one access provider; and

means for denying access by the access requestor to the access provider when a number of connection transactions initiated by the access requestor exceed a configurable threshold number during a first configurable period of time.

16. The system of claim 15, wherein the means for monitoring includes:

means for detecting connection transactions initiated by the access requestor;

means for counting the number of connection transactions initiated by the access requestor during the first configurable period of time; and

means for comparing the number of connection transactions initiated by the access requestor during the first configurable period of time to the configurable threshold number.

17. The system of claim 15, wherein the means for monitoring includes:

means for detecting connection transactions between at least one Internet protocol address and the access provider;

means for counting the number of connection transactions initiated by the Internet protocol address during the first configurable period of time; and

means for comparing the number of connection transactions initiated by the Internet protocol address during the first configurable period of time to the configurable threshold number.

18. The system of claim 17, wherein the means for monitoring includes means for monitoring a computer system for connection transactions made using TCP.

19. The system of claim 17, wherein the means for detecting includes:

means for identifying the Internet protocol address through the use of a header attached to a message representing the connection transaction being detected.

20. The system of claim 15, wherein the means for denying access includes:

means for denying access to the access provider by the access requestor for a second configurable period of time.

21. The system of claim 20, wherein the means for denying access further includes:

means for resetting the second configurable period of time after detecting a new connection transaction initiated by the access requestor during the second configurable period of time.

22. The system of claim 15, wherein the means for denying access includes:

means for denying access to the access provider by the access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

23. The system of claim 15, wherein the access requestor is a client and the access provider is a host such that the means for monitoring includes:

means for detecting connection transactions between at least one client and at least one host.

24. The system of claim 15, wherein the access requestor is a client and the access provider is a host such that the means for monitoring includes:

means for detecting connection transactions between the access requestor and a plurality of access providers.

25. A system for securing an accessible computer system, comprising:

a monitoring component that is structured and arranged to monitor a computer system for connection transactions between at least one access requestor and at least one access provider; and

a blocking component that is structured and arranged to deny access by the access requestor to the access provider when a number of connection transactions initiated by the access requestor exceed a configurable threshold number during a first configurable period of time.

26. The system of claim 25, wherein the monitoring component comprises:

a detection component that is structured and arranged to detect connection transactions initiated by the access requestor;

a counting component that is structured and arranged to count the number of connection transactions initiated by the access requestor during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the access requestor during the first configurable period of time to the configurable threshold number.

27. The system of claim 25, wherein the monitoring component comprises:

a detection component that is structured and arranged to detect connection transactions between at least one Internet protocol address and the access provider;

a counting component that is structured and arranged to count the number of connection transactions initiated by the Internet protocol address during the first configurable period of time; and

a comparing component that is structured and arranged to compare the number of connection transactions initiated by the Internet protocol address during the first configurable period of time to the configurable threshold number.

28. The system of claim 27, wherein the connection transactions include connections made using TCP.

29. The system of claim 27, wherein the detection component comprises:

an identifying component that is structured and arranged to identify the Internet protocol address through the use of a header attached to a message representing the connection transaction being detected.

30. The system of claim 25, wherein the blocking component comprises:

an access preventer that is structured and arranged to deny access to the access provider by the access requestor for a second configurable period of time.

31. The system of claim 30, wherein the blocking component further comprises:

a timing component that is structured and arranged to measure the second configurable period of time during which the access preventer denies access to the access provider by the access requestor.

32. The system of claim 31, wherein the blocking component further comprises:

a reset component that is structured and arranged to reset the timing component after detecting a new connection transaction initiated by the access requestor during the second configurable period of time.

33. The system of claim 25, wherein the blocking component comprises:

an access preventer that is structured and arranged to deny access to the access provider by the access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the access requestor.

34. The system of claim 25, wherein the access requestor is a client and the access provider is a host such that the monitoring component comprises:

a detection component that is structured and arranged to detect connection transactions between at least one client and at least one host.

35. The system of claim 25, wherein the access requestor is a client and the access provider is a host such that the monitoring component comprises:

a detection component that is structured and arranged to detect connection transactions between the access requestor and a plurality of access providers.

36. The system of claim 25, wherein the monitoring component and the blocking component are included in a host computer system that receives communications from a switch.

37. The system of claim 25, wherein the monitoring component and the blocking component are included in a switch that receives communications from a host computer system.